GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1706
TO BE ANSWERED ON: 27.07.2016

CYBER ESPIONAGE

1706 SHRI SUMEDHANAND SARSWATI:
SHRI OM PRAKASH YADAV:

Will the Minister of Electronics and Information Technology be pleased to state: -

(a) whether the Chinese Cyber espionage group DANTI attacked the Indian cyber space;

(b) if so, the details thereof; and

(c) the measures being taken to check such cyber espionage?

ANSWER

MINISTER OF STATE FOR MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI P.P. CHAUDHARY)

(a) and (b): There have been attempts from time to time to penetrate systems/devices of cyber networks operating in Government and its personnel. These attacks have been observed to be originating from the cyber space of a number of countries including China. It has been observed that the attackers are compromising computer systems located in different parts of the world and use masquerading techniques to hide the identity of actual system from which the attacks are being launched. During the current year, incidents of malware infection on certain systems of National Informatics Centre (NIC) network were detected and remedial measures taken. Actions have been initiated by NIC to prevent recurrence of infections. A report has been published on Internet in May 2016 regarding cyber attacks by Danti Group with similar malicious infection patterns.

(c): In order to enhance the cyber security posture of the country and check cyber espionage, the following key actions are being pursued:

i. Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
ii. The Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks.
iii. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers on regular basis. Security tips have been published to enable users to secure their Desktops and mobile/smart phones. Tailored alerts are sent to key organisations to enable them to detect and prevent cyber espionage.
iv. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.
v. NIC protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies. NIC has deployed security solutions including

firewalls, intrusion prevention systems and antivirus solution. Additionally, periodic security audits of resources are performed followed by subsequent hardenings. These are complemented by round-the-clock monitoring of security events and remedial measures are carried out for solving the problems subsequently. A 24x7 security monitoring centre is in place at NIC, for detecting and responding to cyber security incidents.

****